SIGMA Insight

Personal Data Protection in the Age of GDPR

SIGMA Marketing Insights' Guide to Compliance in 2020 and Beyond

SIGMA
MARKETING INSIGHTS

Introduction

In 2018, the European Union enacted a regulation on the protection and use of personal data entitled the *General Data Protection Regulation*, or GDPR. It stands out as the most comprehensive and optimistic attempt to protect consumer data in the digital age. It establishes strict rules for data processing, details citizen's rights regarding their data, and envisages a penalty structure for companies that act carelessly or in bad faith. Most importantly, this law started a conversation on data privacy that resonates globally, and which has already spawned the first American privacy bill, the *California Consumer Privacy Act*, or CCPA.

If you work with consumer data, there's a good chance you're already familiar with common privacy practices, and the potentially catastrophic consequences of a breach. The GDPR and CCPA raise the stakes and are likely the first wave of an oncoming tide of similar laws. *SIGMA Marketing Insights* is here to help you navigate these uncharted waters, and implement best practices across your enterprise. We'll show you how to protect your company and your customers, and how to grow your business in the age of GDPR.
We are committed to your success.

We are providing this *Insight* as a framework for companies like yours to use as they consider the impact digital privacy laws have on their business models.
It is your high-level roadmap to compliance.

History

The GDPR is a replacement for the 1995 *Data Protection Directive* in Europe. This earlier attempt to safeguard privacy enjoined member nations to create local privacy and protection laws that complied with the directive, and was written before the current "digital age." The directive didn't relate to—and was not easily scaled/scoped to cover—key elements of today's data collection, storage, and transfer methodologies. Moreover, it was non-binding, so there was no way to enforce compliance across nations or to punish non-compliance.

The GDPR is both broader and more sophisticated in scope, legally binding, and not modifiable by member nations—either nations comply or they do not. Unlike its predecessor, it is largely built for the digital age, and the electronic management and use of consumer data. It also embraces a key idea: a person's data should be held sacrosanct by the possessor. It should be safeguarded to the limits of the day's technology, and shouldn't be held and used secretly. The GDPR mandates every citizen has explicit ownership of his or her data and must be able to control its use, correct it when it is wrong, or remove it from public use.

There have been many publically-disclosed breaches of information systems in recent years, which have exposed more and more private data to bad actors. For each known breach, there are more undiscovered breaches already in progress. The GDPR is both a reaction to what has already been discovered and an attempt to mitigate future damages.

The upcoming California Consumer Privacy Act (CCPA) is modeled in many respects after the GDPR, and embraces the same idea: personal data should be treated as a sacred object, and even secondary possessors must be accountable for its use and care. Together, these acts demand mindfulness on behalf of any data holder, regardless of why they hold it, for how long, or for what purpose.

It is unlikely that any regulation, no matter how thoughtfully designed, can cure the misuse of consumer data by bad actors. So the next best tool to combat that problem is to assign control of personal data to the person. There has long been an implicit concept that people own their digital data, but in the absence of consumer-ready tools and legal oversight, individuals had no actual control.

Thus, in addition to clear regulations to help companies collectively protect the person—and impactful punishments for those who don't or won't comply, GDPR and CCPA transform individuals into a controlling link in the chain of custody.

"One could argue that people should be smart enough to know that their information doesn't just sit on a paper form in the file of the office where it was completed, but one intent of the law is that a person shouldn't have to "know" from intuition or logic. They should be told, and then protected by the same privacy regulations as the companies they already knew about."

Exploring The Laws

What are the most salient points of each regulation?

Both regulations are built around the same key concepts:

- ***Protection of Personal Info*** — compelling companies to make all reasonable efforts to safeguard personal data; doing what is technologically possible, and supporting it with robust, diligently enforced policies.
- ***Transparency*** — making sure a person knows who has his or her data, and what is done with it.
- ***Control*** — letting the person decide how and when data is used — if it is used at all — and letting a person correct bad data.
- ***Remedy for Misuse*** — guaranteeing that a person has legal recourse when the regulations are breached. This includes paths to financial punishments for noncompliance and monetary compensation to the affected person.

Transparency has the potential to be the most impactful item on the list in the early days of companies learning to comply, especially for third-party processors. In general, consumers know when they have given information to companies, by opening a charge account, purchasing goods, signing up for a newsletter, creating an Apple/iTunes ID, etc. When we look at rules about positive consent, those actions arguably apply. However, when one of those companies decides to engage a third-party, like a marketing firm or printer, those actions weren't preceded by positive consent. In fact, the consumer likely doesn't know the information was shared beyond the original vendors' digital walls. For many people, marketing firms, printers, auditors, are invisible entities to them. So when people think about who holds their data, they likely know Apple has it, their banks have it, Goldfish Fanciers of Chicago has it, but they have no idea John's Digital Marketing Company even exists.

One could argue that people should be smart enough to know that their information doesn't just sit on a paper form in the file of the office where it was completed, but one intent of the law is that a person shouldn't have to "know" from intuition or logic. They should be told, and then protected by the same privacy regulations as the companies they already knew about.

Where are these regulations in effect?

The GDPR is already in effect in all countries that are part of the European Union and extends into European Economic Area countries, such as Iceland, Lichtenstein, and Norway. CCPA isn't in effect anywhere yet, but it fast approaching for California in January 2020. Similar regulations are likely to start dotting the US landscape soon after that.

For a company in the US, what protocols and protections should they already have?

Most companies consider data and system security of paramount importance. Although there is now more focus on personal data privacy and protection, it has long been in the best interest of all companies to safeguard against breaches. They are costly and can be a potentially fatal blow. SIGMA has never had a client who doesn't stare long and hard at what we are doing to protect ourselves, and by extension, their business. We share our security policies and documentation, and undergo third-party audits and share those results. We describe in detail how we protect data at rest and in motion.

Exploring The Laws

What does that mean for GDPR and CCPA compliance?

Well, if your company is taking care of itself, not much new in terms of protection. If you are diligently protecting your data and systems, then you are largely already compliant with the spirit of the regulations. There are some tweaks and different ways of thinking that we'll all need to enact to move from almost-compliant to compliant, but they shouldn't be pain points for any highly-functioning company.

But what about the other goals of the regulations? This is where the work lies.

Who should know the details?

As a matter of course, everybody should know about their companies' privacy and security practices. Security is everyone's business, and responsibility for keeping the company safe does not rest solely on the shoulders of the IT team. It may not be practical for every employee to know everything about security, but all employees should know the basic rulesets of privacy and compliance. At some point, nearly all employees touch some piece of sensitive information, and they need to actively safeguard it when it's in their possession. Because, under GDPR and CCPA, accidental breaches and losses can be punished just as harshly as deliberate actions that flout the laws.

How does GDPR/CCPA shift the focus of data protection to include consumers?

Since personal data is only one kind of data companies manage, it's often protected by tools companies implement by default. But most customers have no idea who really has their data. It's important to note that neither GDPR nor CCPA require companies to scour their data warehouses and actively reach out to every consumer contact they find to announce, "Hey, we have some data on you." That would be a logistical nightmare, and because of the potential cost of doing it, maybe even an existential one. But the regulations DO insist that consumers be given new tools to manage their personal data.

"As a matter of course, everybody should know about their companies' privacy and security practices. Security is everyone's business, and responsibility for keeping the company safe does not rest solely on the shoulders of the IT team."

Consumers need ways to ask companies what data they've stored and how it's being used. They need ways to correct it, opt-out of specific uses, or ask to be forgotten. And they need to be protected so that exercising any of those enumerated rights doesn't result in retribution from affected businesses – they shouldn't lose access to discounts and promotions, or be charged more for goods and services, or be denied service because they opted out.

There is a huge emphasis placed on punishing companies that act in bad faith. Cynics will tell you that not all companies are good citizens; they can be cutthroat and borderline unethical, and make enough money to not care about the complaints of a single consumer. The regulations force them to care by attaching substantial financial penalties for companies that abuse their position as data holders. That's a potent motivator for every company to let consumers determine their own data's fate, and to ensure that they are always behaving in the

best interest of that consumer's data.

What's on the horizon?

GDPR has been in place for a year now, and companies doing business in the EU have been hard at work for even longer to get compliant. American businesses without dealings in the EU were insulated to the point that many likely didn't even reflect on their security practices. The CCPA brings home the need for reflection, and even though it's California-specific, portends the eventual march of all states to similar consumer protections. So what's on the horizon? Probably lots of similar state regulations and a lot of work, starting with serious and deliberate self-assessment.

In 2019, companies need to test themselves against these regulations. How do they get data, and how do they use it? Who do they share it with, and how do they protect it? Can they comply with a remediation or removal request? And how do the companies they work with—third-party processors, printers, et al—answer these questions?

Compliance doesn't stop with the company a consumer already knows has his or her data. Every entity in the chain of custody must be secure and abide by these rules. The regulations go so far as to suggest that compliant companies only do business with other compliant companies, and create their contractual agreements accordingly. Moreover, when it comes to a person exercising their rights under the regulations, any data holder in the chain has the responsibility to inform all other entities in the chain about a request, so that all can take appropriate action. It's safe to assume that this will hold true for future regulations, and it's understandable. Even though companies may be siloed legal entities, they work in concert with one another and often share the very data the regulations aim to protect. It would violate the spirit of the act if any company got a "right to be forgotten" request and simply purged the data from its systems without informing their printer, or the client they received it from, that they'd been asked to remove it.

Next, companies need to take material steps in support of the new framework. The regulations recommend the creation of new company positions, the development of new web pages and privacy language, new interactive forms and contact methods for consumers to use, and, of course, remediation on any systems, processes, or policies that are found to be insufficient to support GDPR and CCPA. They even recommend new language in contracts, and long talks with business partners to understand their readiness to comply, or their ongoing preparations.

Ultimately, it may not be enough for a company to declare itself compliant—especially if they've done all the analysis and mitigation work internally, with resources who are themselves just learning the regulations. Companies should consider reaching out to outside experts and auditors—especially organizations that already have experience with breaches and adjudication of claims against companies who have failed to honor the GDPR.

What about the cost? Unfortunately, this is not a cost-free exercise. Even if your organization does all the work with staff on hand, and you minimize writing checks to auditors and experts, there is still labor cost, and possible infrastructure cost. Companies need to be prepared to take that hit, because the legal and punitive costs of non-compliance can be much, much larger.

Rebuilding the Future

***Disclaimer**: What follows isn't meant to be a comprehensive to-do list. It's a basic framework to familiarize readers with the broad-stroke actions most companies will need to take to get into compliance with GDPR and CCPA. Like most things, the devil is in the details, and great care is needed as companies walk the path to compliance. Companies that aren't able to manage the details themselves should reach out to companies like SIGMA Marketing Insights for help.*

If you've read this far, you probably realize that you have quite a bit of work ahead of you. But you're still not sure how to translate what you've read into concrete action items. You're not alone. Learning what the regulations say and determining what parts apply to your company is the first step; creating and executing a compliance plan is the next.

"Okay," you say, "let's write a bunch of policies and draft a DPO."

But don't. Not yet. You've got a grasp on the regulations, but do you have all the fundamental knowledge you need about your organization? Because you'll need it, and who you are in the organization might even determine how much research you'll need to do before you can take action. At the heart of your efforts is your company's "data playbook". If your company is like many others, you'll probably find a cache of data and security policy documents, ERDs (Entity Relationship Diagrams) for your databases, process flow charts, etc. This is your starting point. If you're lucky, these things are all stored in some logical, easy to navigate taxonomy; otherwise, you'll want to create one, because what you build here will need to be audited and maintained long after this initial effort is over.

Each time a new state/province/country adopts a privacy regulation, each time an existing one changes, and each time someone challenges or asks you to verify your practices, this is where you'll start. At SIGMA, we're in the lucky group – we have been documenting and maintaining for years, so our startup tasks were easily managed and relatively quick. Once you've gathered this documentation, it's time to audit.

> *"Ultimately, it may not be enough for a company to declare itself compliant – especially if they've done all the analysis and mitigation work internally, with resources who are themselves just learning the regulations. Companies should consider reaching out to outside experts."*

The GDPR and CCPA are all about protecting the consumer. As mentioned in the previous section, the strongest base protections come from policies and procedures companies probably already have in place. Most of them are common-sense best practices – like requiring users to have passwords, and granting system access only to those who need it for their job. Some are a little less obvious unless you work in the IT space – like encrypting files before you transmit them to another party, and only transmitting them via secure channels. Some are pretty jargon-y, like "policy of least privilege" and "access control list" and "intrusion prevention system."

The key point, though, is that compliance with the regulations is all-encompassing, and requires you to re-conceive consumer data as

Rebuilding the Future

an entity with a lifecycle. As you start to look at the documentation you've collected, you need to envision a consumer record moving through your company: you should be able to follow it as it enters on a spreadsheet or via some API call, gets cleansed and loaded, assessed, grouped and segmented, output for whatever purpose, and finally removed from your system. Everything you build or tweak from that concept forward will (need to) ensure that you're protecting that data, and can act on it when required. Now it's time to start auditing in earnest.

Step 1 – Document and Audit

How does data come to your company? Here at SIGMA, we obtain data through any number of modern and not-so-modern methods: there are flat files (Excel documents, CSVs) sent to us via secure FTP sites; there are data streams that come in via trusted API calls; there are records that come via direct database replication. This is the entrance point of the data lifecycle we described above. Now look at how your company does it: does data enter securely? Or are your clients and data suppliers sending unencrypted word documents via email, FYI-copied to 10 people? No matter which answer it is, you'll need to document it. Don't worry about fixing it yet – just get a handle on it.

Then move on to the next question: how does data move through your company? Document this, and then repeat for who has access to this data, how are you using it, who are you sending it to, etc.?

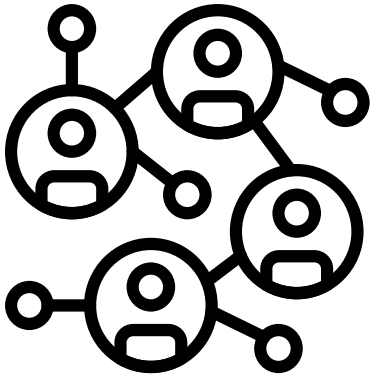
Follow that lifecycle until you can account for where consumer data is at any time, and who can see it, and what you're doing with it. That map you've just drawn will highlight where you need to place additional controls, and what policies need to be amended or created, and will eventually show you how to respond to the inevitable data removal or remediation requests you'll get. If you don't have what you need internally to complete this audit, hire an expert.

Companies that miss the mark on this first fundamental step are the ones most likely to struggle with remediation actions later, and possibly end up writing checks to damaged consumers. Once you're done here, you're finally ready to take some action.

Rebuilding the Future

Step 2– Build Your Team, Appoint a DPO

During the documentation and audit stage of your privacy project, you'll most likely engage a cross-functional team of IT, security, and account people, and maybe an executive or two. If you haven't formalized them into a data privacy team, you should.



Making wholesale policy and process changes requires people all across your organization, and someone needs to provide ongoing oversight since new regulations are already queuing up as you build what you're building. Follow the GDPR recommendation and appoint a Data Protection Officer (DPO). He or she will lead the privacy team, and be the everyday expert on how your company complies, and what needs to change tomorrow to stay compliant. The DPO doesn't need to come from any particular level/discipline within the organization, but he or she will need to develop a formidable knowledge base on all things compliance, and a complete understanding of all those "who, what, where, how" questions you've answered about the data lifecycle. The DPO will become the public face of your data privacy efforts.

Step 3 – (Re) Create Your Data Security Model

The privacy team did a lot of research before; now it's time to plan a management and mitigation strategy – caring for the data coming into, residing on, and leaving your systems. Remember, the goal here is to ensure that consumer data is protected no matter where it is. At this stage, you'll most likely need to tweak or write policies that dictate:

Access to Data

Who can see this data as it moves through your systems? SIGMA uses the policy of least privilege, and an explicit access request process. Every system has a knowledgeable data owner who reviews access requests and ensures that only those with a business need can see data. This applies to FTP sites, file shares, databases, email accounts, et al. If the data can rest or pass through a location, only authorized people should be able to see it or do anything with it.

Data Transmission

How does data enter and leave your company, and how does it traverse systems? SIGMA always uses secure transport, and will often supplement with file-level, private key/public key encryption. Remember that your company is responsible for the data both on the way in, and on the way out.

Comprehensive Monitoring

Who touches data, when, and why? Part of demonstrating compliance is tracking/documenting what happens to data; It might seem excessive if you already have the right controls in place, but think of any audit your company performs: compliance has always been a matching set of creating a control, and proving the control is being used. Just having a

control in place is useless without testing and documentation – California, the EU, and probably all of your clients, won't take your word for it. And they shouldn't.

Endpoint Security

How do you protect your systems from breaches?

It's not enough to encrypt outgoing files, create the right access control request forms and policies, and write out log files that show who's touching what. You also have to protect your network from intrusion. Under the GDPR and CCPA rules, any breach that stems from a failure to properly secure your network can be treated like a deliberate act and punished the same way. In practical terms, that means you'll need physical security for your data center, firewalls and intrusion prevention systems, anti-malware programs, real-time monitoring and remediation, encrypted laptops, and still more logging. Your network has to be hardened against hackers and malware and should be regularly and rigorously tested.

Ethical/Approved Use

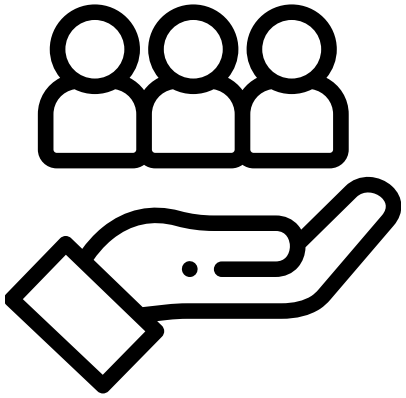
What does your company do with consumer data? Another key requirement of both data privacy acts is ensuring that data isn't misused. At the highest level, this one can start with some new language in your contracts. Ensure that SOWs and MSAs detail in plain, succinct language what your client requires of your company as it pertains to data.

Required Data

What data does your company need to do its job? It may seem counter-intuitive to limit the data a client wants to provide, but there is inherent protection for the consumer if companies limit what they get. Don't need a credit card or bank account numbers? Don't need SSNs? Then don't get them, or at least encrypt or obscure them in a meaningful way. If there is a breach, it's that much less data that has been spilled into hacker hands.

Data Destruction

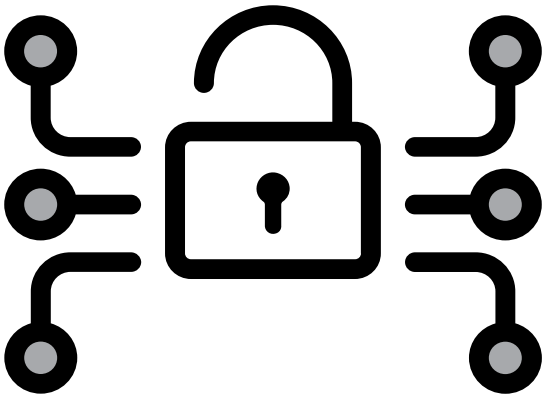
How does your company remove data at the end of a contract, or whenever a client asks you to? This one requires heavy lifting in IT, but the ability to securely dispose of data is of critical importance for any company. The federal government is one of many entities that prescribe how companies should wipe data. Learn the rules and best practices, and detail how to follow them.



Rebuilding the Future

Step 4 – From Plan to Action: Implement Your New Controls

Okay, so you've done a ton of research and writing, and have a handful of new policies, some awesome process documentation, and maybe even a wiki that details all your privacy practices. Now it's time to implement and test.



If you've followed the basic path here, your system security should tighten up nicely with each implementation step. You're not compliant with either regulation yet, but you've created a strong foundation for both of them, just by improving the overall health of your company. Get your new controls in place, publish your policies, and test, test, test. Make sure that what you've written in policy form, works in practice.

Step 5 – Empower the Consumer

Your network is secure. Data is flowing in and out in the best ways possible. You're only getting what you need, logging who touches it, and obliterating it permanently when it's no longer needed. That superstructure is now ready to support data transparency and consumer controls.

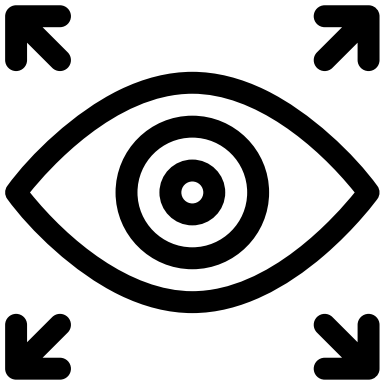
Under the GDPR and CCPA, consumers have some new/enhanced rights. At any time, they can demand disclosure of whatever information a company has about them. They get to direct how companies use that info, and how. They get to repair it if it's faulty, and they get to make it disappear on demand. So the next step is to enable those consumer controls.

Both laws direct companies to create new channels to grant clients clear, easy access to your data privacy team: toll-free phone numbers, easy-to-find email addresses, and new web pages with forms that don't require any kind of signup or account activation. You need to create all of those. The CCPA outlines specific language for pages on your site, and website navigation pathways that all compliant companies must follow.

The laws require more than one mechanism for consumers to reach companies with their data privacy requests, such as a phone number AND an email address. Get these in place and you are almost ready to call yourself compliant.

Rebuilding the Future

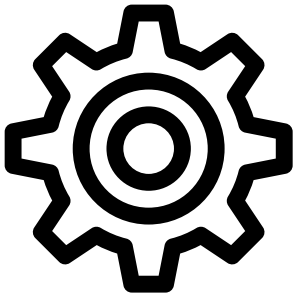
Step 6 – Your Response and Action Methodologies at Play



GDPR and CCPA require companies to act on data requests in several critical ways. There are time limits for each step in the process, an "official" format companies must use when sharing data with its owners, rules on how to vet a requester, and even what constitutes a valid request. But these requirements aren't outrageously burdensome – they shouldn't represent any threat to your business.

Yes, the onus is on companies to comply, and there is an ongoing cost associated with data privacy requests, but both laws recognize that assisting a consumer can pose some serious challenges. It won't always be possible to give the consumer everything he or she wants or respond as quickly as the laws require. So the authors created common-sense exemptions/exceptions to protect affected companies from unacceptable/damaging resource and monetary costs; and also to protect them from capricious actors on the consumer side of the equation. Companies must make all reasonable attempts to comply with requests, but aren't expected to bankrupt themselves or take actions that are deleterious to their overall corporate health. Companies should acquaint themselves with these provisions as they build their privacy practices, and take full advantage of the protections they provide.

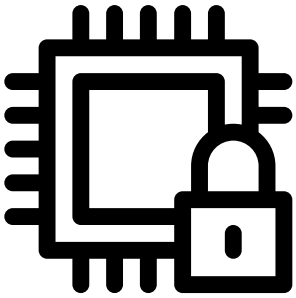
Another critical requirement is for all companies within the chain of custody to communicate with each other. A data privacy request anywhere in the chain should be treated as data privacy requests everywhere in the chain. Companies must communicate with their partners, and work in concert to comprehensively cascade the consumer's control choices. This will be key to creating a successful program, and to ensure the future of your company in the new digital privacy landscape.



Finally, you need to show your work. Just like eighth grade math class, it isn't enough to simply say you're done. You need to prove that you've honored a data privacy request; that means copious documentation, some that goes directly to the consumer, and more that you'll store internally for future auditors and legal challenges. Inasmuch as your privacy controls are the foundation of success in the GDPR/CCPA, a quality "paper trail" is the actual public measure.

Rebuilding the Future

Step 7 – Protect the Custody Chain, Protect the Consumer



In addition to the solid directives in the GDPR and CCPA, there is an explicit suggestion that needs reinforcing. It's critical that your company becomes a good citizen of the digital future and complies materially in protecting the consumer. We've discussed sharing data privacy requests with all members of the chain of custody, but there's also a kind of socio-financial pressure that compliant companies need to bring into the changing corporate landscape – they should only do business with compliant partners. Remember the old aphorism about how a chain is only as strong as its weakest link? It applies here, and it's up to compliant companies to eliminate those weak links by denying non-compliant companies a spot in the chain.

That means evaluating all business partners across this new dimension of data privacy. Is that potential vendor who's courting you compliant? Are they working to be? Is your new data processor ready to honor a takedown request? What's their roadmap?

In the nascent days of GDPR adoption here in the US, and while the ink is still drying on the CCPA, it's imperative to see that all your partners are at least working towards compliance. When you talk with them, ask for their roadmaps. When you write their next contracts, include compliance as a consideration. Make sure your data chain partners are doing the same thing you are. If you're lucky, some of them will already be compliant. But keep the conversation going. Right now, achieving that first moment of compliance is a goal all ethical companies should have, even if they are just starting the race.

Once 2020 rolls around, you owe it consumers, and your company, to start excluding those non-compliant partners entirely. That's the socio-financial pressure I alluded to above. The regulations want to make it impossible for non-compliant businesses to stay afloat in the new data sea. Your company is one of what should be many enforcers. In 2020, you shouldn't sign or write any contract that doesn't include data privacy terms that align with GDPR and CCPA.

Personal Data Redefined

*Under the GDPR, the definition of **personal data** has been expanded to include new ways of identifying individuals, such as IP addresses and biometric data. **Article 4** of the GDPR defines it as:*

> *"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

Businesses need to assimilate this new definition as they create their controls, and ensure that their protection models cover all the newly designated facets of personal data.

The Future

It's critical to understand that compliance is a living, breathing, and evolving thing. If you've done everything discussed here – put in due diligence to really learn the regulations, enacted new controls, created your privacy sites and toll-free phone number (with someone to answer it!), developed your output and data remediation certifications, etc. – then, you can take a deep breath, and maybe raise a celebratory glass. You're protecting consumers (and yourselves) better than you have before and joined a club of secure, ethical companies who are best equipped to survive as the privacy landscape evolves. But remember: compliance is that rare entity which exists both as a point-in-time validation of your work, and a journey to the future.

You need to stay abreast of changes in the existing laws, attend the birth of new laws, and discern all the implicit impacts that exist in the gray spaces between yesterday's rules and tomorrow's. Your company needs to evolve continuously; data privacy must become a part of your DNA, and perhaps even a dedicated practice at your shop. These practices will reiterate countless times, and in the same way you had to be diligent in your startup, you'll need to stay diligent in your upkeep.

Consumers have a rougher time today than ever. So many unnamed actors have their information, so many bad actors want to harm them, and every ethical seller wants their business. There is a virtual onslaught of touches in their everyday lives, and it's harder and harder to tell a legitimate marketer from a Nigerian Prince. Commerce lives on information – that's why we trade it, explore it, enhance it. Now it's time to protect it, and to give consumers the benefit of our combined strength as we usher them deeper and deeper into the digital millennium...and beyond.

For help getting your company GDPR and CCPA compliant,
contact SIGMA Marketing Insights at:
GetCompliant@sigmamarketing.com

Transforming Business | Through Data

About the Author

Frank Sanseri

is the Director of IT and Data Protection Officer for SIGMA Marketing Insights.
With over 20 years experience in information technology and related fields, Frank is an expert in data protection and system security, and is the chief architect of SIGMA's compliance program.

You can write to him at frank.sanseri@sigmamarketing.com

About SIGMA Marketing Insights

For over 30 years, we've been cleaning, analyzing, modeling, and interpreting data to design actionable strategy and marketing plans – across all your channels.

This experience means we are here to help you understand the connection between your data, your marketing strategy, and your customers. From campaign development to implementation, we believe in dispelling the mystery of data and maintaining strength across all marketing channels.

Visit us on the web at: https://www.sigmamarketing.com

All icons provided by FlatIcon: https://www.flaticon.com